制定日:2009/08/19

別紙－１「安全管理の基準」

①運用管理

対策番号	項目		対策		管理レベル 1	2	3	対策についての定義している規程類
1-1	個人情報の取扱ルール							
1-1-1		個人情報を正しい手順で処理する	－	処理手順を定めるに際しリスク分析を行い、リスクの軽減を図る	○	○	○	『個人情報特定管理規程』、及び『個人情報リスクアセスメント規程』に従う
1-1-2			－	標準作業の処理手順を業務運用マニュアル等で定める	―	○	○	『個人情報安全管理規程』に従う
1-1-3			－	例外処理（処理手順が定まっていない業務処理）の必要性が生じた時の業務手順を業務運用マニュアル等で定める	―	○	○	『個人情報安全管理規程』に従う
1-2	事故対応							
1-2-1		事故発生時に適切に対処する	－	『個人情報問題処理規程』に定められた処理手順（報告、是正処置、類似事故の点検）を関係者に周知する	○	○	○	『個人情報インシデント規程』に従う
1-2-2			－	定期的に（目安:１回／年）事故/障害時の対応訓練を行う	○	○	○	『個人情報インシデント規程』および『個人情報教育訓練規程』に従う
1-2-3		再発防止対策を行う	－	事故発生後、再発防止対策を策定する	○	○	○	『個人情報是正処置・予防処置規程』に従う
1-3	適正な管理の維持							
1-3-1		個人情報の管理責任を明確にする	－	管理の責任者を定める。	○	○	○	『個人情報特定管理規程』に従う
1-3-2		管理状況を点検する	－	業務運用マニュアル等に定めた運用ルールを遵守して業務を遂行していることを、定期的（目安:１回以上／年）に監査する。例外処置を定めている場合は、その妥当性について再	○	○	○	『個人情報内部監査規程』に従う
1-3-3		教育する	－	当該業務に関連する管理職、社員、派遣社員に対し、上記運用ルールを教育する	○	○	○	『個人情報教育・訓練規程』に従う
1-4	受託元と契約							
1-4-1		受託元と契約を締結する	－	受託元と契約を締結し、個人情報の利用範囲を明らかにする。 ※受託(再請負)の場合は不要	○	○	○	『個人情報取得・利用・提供規程』に従う
1-5	委託先と契約							
1-5-1		業務委託先を選定する	－	「個人情報委託管理規程」に従い、個人情報の預託先を選定する。	○	○	○	『個人情報委託管理規程』に従う
1-5-2		業務委託先と契約を締結する	－	「個人情報委託管理規程」に従い、個人情報の預託先と契約を締結する。	○	○	○	『個人情報委託管理規程』に従う
1-5-3		業務委託先を点検する	－	「個人情報委託管理規程」に従い、個人情報の預託先の定期点検を行う。	○	○	○	『個人情報委託管理規程』に従う
1-6	提供先と合意							
1-6-1		提供に関して承認を得る	－	「個人情報取得・利用・提供規程」に従い、提供の申請を個人情報保護管理責任者に対して行い、承認を得る。	○	○	○	『個人情報取得・利用・提供規程』に従う
1-7	システム開発・変更							

1-7-1		運用環境のセキュリティが損なわれないことの検証	－	情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれないことの検証	○	○	○	『個人情報技術的安全管理細則』に従う
1-7-2		テストデータとして個人データを利用することの禁止	－	情報システムの動作確認時のテストデータとして個人データを利用することの禁止	○	○	○	『個人情報技術的安全管理細則』に従う
1-8	個人情報本人と合意							
1-8-1		個人情報本人への告知文の内容を業務責任者が確認する。	－	個人情報本人に対して利用目的等を告知する際の告知文の内容を、記載する。業務責任者は、告知文の内容を確認し、問題があれば修正を指示する。 ※受託の場合は不要	○	○	○	『個人情報情報相談・開示規程』に従う
1-8-2		利用目的等を個人情報本人に告知する	－	取得を行う前に、個人情報本人に対して利用目的等を告知する ※受託の場合は不要	○	○	○	『個人情報取得・利用・提供規程』に従う
1-8-3		個人情報本人から同意を取得する	－	取得を行う前に、個人情報本人に対して利用目的等に対して、書面等により同意を得る ※受託の場合は不要	○	○	○	『個人情報取得・利用・提供規程』に従う

②入出力管理

対策番号	項目		対策		管理レベル 1	2	3	対策が記述してあるマニュアル類
2-1	正確な入力							
2-1-1		入力漏れを検出する	個人情報本人の入力	個人情報本人が直接入力する場合、必要な入力項目の入力実行をチェックする。	○	○	○	『個人情報技術的安全管理細則』に従う
2-1-2			入力担当者の入力	取得側の入力担当者が入力する場合、入力元の情報と入力結果の数および必須入力項目などのチェックを行う。	○	○	○	『個人情報技術的安全管理細則』に従う
2-1-3		入力誤りを防止する	個人情報本人の入力	個人情報本人が直接入力する場合、登録前に入力結果を確認する手段を用意する	○	○	○	『個人情報技術的安全管理細則』に従う
2-1-4			入力担当者の入力	取得側の入力担当者が入力する場合、何らかの誤りを検出する手段を実施する。	○	○	○	『個人情報技術的安全管理細則』に従う
2-1-5		他人データへのすりかわりを防止する	－	ID番号、メールアドレス等、個人の特定に利用されるキー情報については、誤りを検出する手段(手順)を実施する。(個人の特定に利用されるキー情報とは、その情報の一部が間違って入力された場合、他人の個人情報と認識される恐れのある情報を言う。)	―	○	○	『個人情報技術的安全管理細則』に従う
2-2	入力情報の修正							
2-2-1		個人情報本人の申告に基づき修正する	－	個人情報本人に対し個人情報の照会窓口を公開する	○	○	○	『個人情報情報相談・開示規程』に従う
2-2-2			－	窓口において適正な修正を受付け、実施する	○	○	○	『個人情報情報相談・開示規程』に従う
2-2-3			－	修正を実施した場合、修正処理の記録をとる	○	○	○	『個人情報情報相談・開示規程』に従う

2-2-4		入力担当者による誤りを復旧する	－	誤り/消失の場合の復旧処置について、業務運用マニュアル等に手順を定める。	○	○	○	『個人情報技術的安全管理細則』に従う
2-2-5			－	修正を実施した場合、修正処理の記録をとる	○	○	○	『個人情報技術的安全管理細則』に従う
2-3	入出力情報の管理							
2-3-1		出力情報を正確に引き渡す	－	預託先／委託先への引渡し並びに預託元／委託元からの引渡しに際し、引渡しの事実を記録する	―	○	○	『個人情報委託管理細則』に従う
2-3-2		アクセス権者による不正な出力を防止する	印刷出力	プリンタ等の出力機器は管理者の目が届く範囲に、置く	―	○	○	『個人情報物理的安全管理細則』に従う
2-3-3			可搬媒体書込装置	可搬記録媒体書き込み装置の利用を管理者が管理する	―	○	○	『個人情報物理的安全管理細則』に従う
2-3-4			DB	個人情報を蓄積しているDB等へのアクセスログを取り、定期的に点検する	―	○	○	『個人情報技術的安全管理細則』に従う
2-3-5			可搬出力媒体	紙、FDなどの可搬出力媒体については、出力記録を取り、廃棄/引渡し記録と照合する	―	○	○	『個人情報物理的安全管理細則』に従う
2-3-6		利用後は個人情報を読めなくする	磁気媒体等	利用後は定められた適切な時期までに個人情報を消去する。 ただし、その媒体を別の業務で使用する場合は、消去ソフトを使用して個人情報を完全に消去する。 その媒体を廃棄する場合は消去ソフトを使用して個人情報を完全に消去するか、あるいは、記録媒体を機械的に破壊する。	○	○	○	『個人情報物理的安全管理細則』に従う
2-3-7			紙媒体等	利用後は定められた適切な時期までに、決められた手順で廃棄方法で廃棄する。廃棄回収場所に置き、廃棄回収者が廃棄文書を回収するまでの放置時間は15分以内とする。	○	○	○	『個人情報物理的安全管理細則』に従う
2-3-8			紙媒体等	利用後は決められた時期までに、利用現場で裁断、廃棄する。	―	―	○	『個人情報物理的安全管理細則』に従う
2-3-9			表示装置	画面等は離席時に表示を消す	○	○	○	『個人情報技術的安全管理細則』に従う
2-3-10			表示装置	スクリーンセーバーによる表示を消す方法を選んだ場合は、解除にパスワードを設定する	―	○	○	『個人情報技術的安全管理細則』に従う
2-3-11		クリアデスク	－	設置されているオフィス機器、及び机上等に文書を放置しない	○	○	○	『個人情報物理的安全管理細則』に従う
2-3-12		端末又はアドレス等の識別と認証の実施	－	個人データのアクセス権限を有する各従業者が使用できる端末又はアドレス等の識別と認証の実施	―	―	○	『個人情報技術的安全管理細則』に従う
2-3-13		端末の限定	－	個人データを入力できる端末の、業務上の必要性に基づく限定	―	―	○	『個人情報技術的安全管理細則』に従う
2-3-14		情報システムへの同時利用者数の制限	－	個人データを格納した情報システムへの同時利用者数の制限	―	―	○	『個人情報技術的安全管理細則』に従う
2-3-15		情報システムへの利用時間の制限	－	個人データを格納した情報システムの利用時間の制限	―	―	○	『個人情報技術的安全管理細則』に従う
2-3-16		アプリケーションの無権限利用の防止	－	個人データにアクセス可能なアプリケーションの無権限利用防止	―	―	○	『個人情報技術的安全管理細則』に従う

2-3-17		端末に付与する機能の限定	－	個人データを利用・加工できる端末に付与する機能の、業務上の必要性に基づく、限定	―	―	○	『個人情報技術的安全管理細則』に従う

③保管/廃棄管理

保管とは、当該データの安全管理に関わる担当者が目が届く範囲から不在になる可能性のある場所に情報・データを半日以上置くこと。

対策番号	項目		対策		管理レベル			対策についての定義している規程類
					1	2	3	
3-1	保管場所							
3-1-1		決められた保管場所へ保管する	－	保管場所を定めて運用する	―	○	○	『個人情報物理的安全管理細則』及び『個人情報技術的安全管理細則』に従う
3-1-2		決められた保管場所から取り出し後及び保管後、記録をとる	－	INPUT(入力／受入)OUTPUT(出力/払出)の保管記録をとる	―	○	○	『個人情報物理的安全管理細則』及び『個人情報技術的安全管理細則』に従う
3-1-3		保管場所からの移動を制限する	物理移動	保管場所から移動する場合は、当該個人情報に関する個人情報管理者の許可を得る。	○	○	○	『個人情報物理的安全管理細則』に従う
3-1-4			通信手段による移動	保管場所がネットワーク接続されたDB等であり、保管場所とは異なる場所から通信手段を用いて個人情報を取り出す場合は、アクセス制御を実施し、アクセス権の付与に際しては業務責任者の許可を得る。	○	○	○	『個人情報技術的安全管理細則』に従う
3-1-5		保管場所を施錠管理する	物理的な持出し対策	保管場所は施錠管理する、あるいはデータそのものを暗号化して保管する。	―	○	○	『個人情報物理的安全管理細則』に従う
3-1-6			物理的な持出し対策	可搬型コンピュータは退社時施錠場所に保管する。	○	○	○	『個人情報物理的安全管理細則』に従う
3-1-7			物理的な持出し対策	紙媒体は退社時施錠場所に保管する。あるいは重要な書類は、管理者自ら施錠管理を実施し、記録管理する	○	○	○	『個人情報物理的安全管理細則』に従う
3-1-8			通信手段によりアクセス可能な場合の対策	保管場所がネットワーク接続されたDB等であり、保管場所とは異なる場所から個人情報を取り出せる場合は、アクセス制御に使用されるパスワード等はそのセキュリティ強度に応じて定期的に変更する。	○	○	○	『個人情報技術的安全管理細則』に従う
3-1-9		保管状況を定期的に点検する	－	保管記録に基づいて定期的に点検し、保管状況を確認する	―	○	○	『個人情報物理的安全管理細則』及び『個人情報技術的安全管理細則』に従う
3-1-10		部外者に見えなくする	－	保管場所/保管庫/磁気媒体等に個人情報の存在が直接的にわかる様な表記をしない	―	○	○	『個人情報物理的安全管理細則』に従う
3-2	データの紛失対策							
3-2-1		アクセス制限を行う	－	アクセス制御を実施し、アクセス権の付与に際しては業務責任者の許可を得る。	○	○	○	『個人情報技術的安全管理細則』に従う
3-2-2		紛失データを再生する	－	二重保管および分散保管をおこなう。あるいはデータを再生する何らかの手段を用意する	―	―	○	『個人情報技術的安全管理細則』に従う
3-2-3			－	一定の周期でバックアップを取得する	―	○	○	『個人情報技術的安全管理細則』に従う

3-2-4		不要利用者IDを削除する	−	もはや必要の無い、利用者IDがないかを定期的に確認し、あれば削除する。	○	○	○	『個人情報技術的安全管理細則』に従う
3-2-5		パスワードを更新する	−	パスワード等は他人に知られないように管理する。必要な場合、セキュリティ強度に応じて定期的(目安:パスワードの場合は1回/6ヶ月)に変更する。	○	○	○	『個人情報技術的安全管理細則』に従う
3-3	保管期間を定める							
3-3-1		保管開始時に保管期限を定める	−	保管開始前に保管期限を取得目的に応じて定める	○	○	○	『個人情報物理的安全管理細則』に従う
3-3-2		不必要になったら廃棄する	−	保管記録に基づいて定期的に点検し、保管状況結果に基づき、保管期限を過ぎたデータや不必要なデータを廃棄する	○	○	○	『個人情報物理的安全管理細則』に従う
3-4	データ廃棄後の安全対策							
3-4-1		確実に廃棄する	−	保管データの廃棄時に廃棄記録を取る。	−	○	○	『個人情報物理的安全管理細則』に従う
3-4-2		データを読めない状態にして廃棄する	磁気媒体等	廃棄時に消去ソフトを使用してデータを完全に消去するか、あるいは記録媒体を機械的に破壊する。	○	○	○	『個人情報物理的安全管理細則』に従う
3-4-3			紙媒体等	利用現場で細断する	−	−	○	『個人情報物理的安全管理細則』に従う
3-4-4			紙媒体等	「秘文書」廃棄の方法を定め、廃棄する。廃棄回収場所に置き、廃棄回収者が廃棄文書を回収するまでの放置時間は15分以内とす	○	○	○	『個人情報物理的安全管理細則』に従う
3-5	バックアップ・復旧対策							
3-5-1		媒体の本社以外での保管	−	個人データを記録している媒体の本社以外での保管	−	−	○	『個人情報技術的安全管理細則』に従う
3-5-2		データが復元できることのテストの実施	−	個人データのバックアップから迅速にデータが復元できることのテストの実施	−	−	○	『個人情報技術的安全管理細則』に従う
3-6	悪意のあるソフトウェア対策							
3-6-1		セキュリティパッチの適用	−	オペレーティング(OS)、アプリケーション等に対するセキュリティ対策用修正ソフトウェアの	○	○	○	『個人情報技術的安全管理細則』に従う
3-6-2		不正ソフトウェア対策の有効性・安定性の確認	−	不正ソフトウェア対策の有効性・安定性の確認	○	○	○	『個人情報技術的安全管理細則』に従う
3-6-3		コンピュータウィルスチェックソフトを最新版にする	−	ワクチンデータ・ソフトがリリースされたたら常に更新する	○	○	○	『個人情報技術的安全管理細則』に従う
3-7	天災							
3-7-1		地震対策の実施	−	サーバラック又はサーバ自体を転倒、転落から防止するために固定する	○	○	○	『個人情報技術的安全管理細則』に従う
3-7-2		火災対策の実施	−	消火器、ハロゲンガスなどの消化装置を整備する	○	○	○	『個人情報技術的安全管理細則』に従う
3-7-3		停電対策の実施	−	UPS等の無停電対策を実施する	○	○	○	『個人情報技術的安全管理細則』に従う
3-7-4		浸水対策の実施	−	浸水しない場所に設置する	○	○	○	『個人情報技術的安全管理細則』に従う

④入退室管理

対策番号	項目	対策	管理レベル			対策についての定義している規程類
			1	2	3	

4-1	個人情報取扱場所への入退者を限定する						
4-1-1	建物への入退館を管理する	－	建物の入退館規則を遵守する	○	○	○	『個人情報物理的安全管理細則』に従う
4-1-2	固定的な入退室資格付与を管理する	－	入退室資格資格付与に関するルールを定めて運用する	－	○	○	『個人情報物理的安全管理細則』に従う
4-1-3		－	入退室許可者を台帳等で管理する	－	○	○	『個人情報物理的安全管理細則』に従う
4-1-4	一時的な入退者を管理する	－	入退館は、受付または守衛にて身元/用件等を確認する	－	○	○	『個人情報物理的安全管理細則』に従う
4-1-5		－	一時的入退者は、臨時の識別証等の認識手段を携帯させる。あるいは、立会人をつけ立入り場所の確認と抑制を行う	－	－	○	『個人情報物理的安全管理細則』に従う
4-2	入退室者の記録管理						
4-2-1	固定的な入退室資格付与者の入退記録を取る	－	鍵機構と連動して自動的に入退者記録を取る。あるいは受付簿等に入退者記録簿を置いて入退者記録を取る	－	－	○	『個人情報物理的安全管理細則』に従う
4-2-2	一時的な入退室者の記録を取る	－	受付簿等に入退者名を記録させる	－	○	○	『個人情報物理的安全管理細則』に従う
4-2-3		－	受付にて入退者の身元/用件等を記録する。あるいは、鍵機構と連動して自動的に入退者記録を取る	－	－	○	『個人情報物理的安全管理細則』に従う
4-3	出入り口の施錠/解錠管理						
4-3-1	鍵の保管/受渡しの記録をとる	手動	鍵貸し出し記録簿を設置して記録管理する	－	－	○	『個人情報物理的安全管理細則』に従う
4-3-2	出入り口を施錠する	手動	開錠キーは管理職が管理する	－	－	○	『個人情報物理的安全管理細則』に従う
4-3-3		機械式	10キーや入退室者識別機構と連動して施錠/解錠を自動的に行う	－	－	○	『個人情報物理的安全管理細則』に従う
4-3-4		機械式	10キー等の場合、定期的に開錠キーを変更する。	－	－	○	『個人情報物理的安全管理細則』に従う
4-4	搬出入物のチェック						
4-4-1	搬出入物を制限する	－	搬出入物に関するルールを定め実施する	－	－	○	『個人情報物理的安全管理細則』に従う
4-4-2		－	受付、守衛あるいは監視装置を置く	－	－	○	『個人情報物理的安全管理細則』に従う

⑤輸送/送受信管理

対策番号	項目	対策		管理レベル 1	2	3	対策についての定義している規程類
5-1	物理媒体による授受/交換時の対策						
5-1-1	授受記録を取る	業務委託	授受に際しては、個人情報の種類/件数、相手先、媒体種別、等を確認し記録する	○	○	○	『個人情報委託管理規程』に従う
5-1-2		業務受託	授受に際しては、個人情報の種類/件数、相手先、媒体種別、等を確認し記録する	○	○	○	『個人情報取得・利用・提供規程』に従う
5-1-3		提供	授受に際しては、個人情報の種類/件数、相手先、媒体種別、等を確認し記録する	○	○	○	『個人情報取得・利用・提供規程』に従う
5-1-4		社内他部門への委託	授受に際しては、個人情報の種類/件数、相手先、媒体種別、等を確認し記録する	－	－	○	『個人情報取得・利用・提供規程』に従う
5-2	物理的輸送路上の対策						

5-2-1		紛失のおそれを少なくする	社外	送付先へ直接手渡しをする、あるいは書留等の受渡し記録のある特別に管理された便を使う	―	○	○	『個人情報物理的安全管理細則』に従う
5-2-2			社内	社内メール便、あるいは送付先へ直接手渡しをする	―	○	○	『個人情報物理的安全管理細則』に従う
5-2-3			社内	社内貴重品メール便、あるいは送付先へ直接手渡しをする	―	―	○	『個人情報物理的安全管理細則』に従う
5-2-4		第三者が見れないようにする	社外	磁気媒体等の場合は、データを暗号化する。	―	―	○	『個人情報技術的安全管理細則』に従う
5-2-5			社外	袋、箱等を用い直接目に触れないようにする	○	○	○	『個人情報物理的安全管理細則』に従う
5-2-6			社内	袋、箱等を用い直接目に触れないようにする	―	○	○	『個人情報物理的安全管理細則』に従う
5-2-7		漏洩を検出する	社外	開封すると痕跡が残る封をして送る	―	―	○	『個人情報物理的安全管理細則』に従う
5-3	電子的送受信路上の対策							
5-3-1		個人情報データを暗号化する。(傍受対策を取る。)	法人ネットワーク内	社内並びに法人のネットワーク内においてメールによる通信において、定型業務として繰り返し送受信を行う場合、あるいは単発的であっても個人情報の集合体のデータを送受信する場合は、送信データの暗号化を行う	―	○	○	『個人情報技術的安全管理細則』に従う
5-3-2			法人ネットワーク内のその他通信	社内並びに法人のネットワーク内においてメール以外の通信において、定型業務として繰り返し送受信を行う場合、あるいは単発的であっても個人情報の集合体のデータを送受信する場合は、送信データの暗号化を行う。	―	―	○	『個人情報技術的安全管理細則』に従う
5-3-3			法人ネットワーク外との通	社内並びに法人と、社外の通信を行う場合、送信データを暗号化するか、機密性の保たれた回線インフラを利用する。	―	○	○	『個人情報技術的安全管理細則』に従う
5-3-4			法人ネットワーク外との通信	業務委託、業務受託において、定型業務として繰り返し送受信を行う場合、あるいは単発的であっても個人情報の集合体のデータを送受信する場合は、送信データの暗号化を行	―	○	○	『個人情報技術的安全管理細則』に従う
5-3-5		送受信行為の一致確認	－	送信項目/件数/日時等に関する送信ログと受信ログの一致を確認する、あるいは、送信内容と受信内容の一致を確認する	―	○	○	『個人情報技術的安全管理細則』に従う
5-3-6		クロスサイトスクリプティングへの対策	－	スクリプトコードが入力されても、入力内容をそのまま表示せずに、スクリプトなどのコードを識別して無効化する	―	○	○	『個人情報技術的安全管理細則』に従う